FARISMUN TOPIC GUIDE

TABLE OF CONTENTS

Meet the Chairs:

Hibah Shabbir

Hello! My name is Hibah Shabbir and I'll be one of the chairs for the UN Human Rights Council at this year's FARISMUN conference! I'm an 18-year-old architecture student from Pakistan who loves politics and debating which is why I've been participating in MUN conferences for the last 3 years. On top of that, I've been a head delegate for 2 years at Al-Faris International School where I helped train delegates and chair mock committees so I'm delighted to be your chair and especially excited to be chairing one of my favorite committees, the HRC.

Yasmin Salman

My name is Yasmin Salman, I am 18 years old and currently studying Business Administration at Al Faisal University. I am an Austrian national but originally from Palestine and I have lived in Riyadh, Saudi Arabia for the past 9 years now. I have previously attended two MUNs that were very informative and helped me grow as a person. My first MUN was DHAMUN which was in Dhahran, Saudi Arabia and I took that as an opportunity to properly observe how a MUN works and what the most efficient way is to be prepared for one. In my second MUN, SAMUN, I decided to participate and was more active during writing the resolutions and coming up with arguments during the debate. I am excited to be chairing the HRC committee in the FARISMUN.

Committee Introduction

The Human Rights Council (HRC) is a body of the United Nations that is in charge of promoting and protecting human rights around the world as well as addressing situations regarding human rights violations. It's also responsible for shedding light on thematic human rights issues and making recommendations.

The Human Rights Council consists of 47 member states which have been elected by the UN General Assembly and they meet in Geneva, Switzerland for at least 10 weeks out of the year. The HRC was created by the United Nations General Assembly on 15 March 2006 by resolution 60/251.

The HRC discusses topics surrounding a variety of human rights issues, such as minority discrimination, human rights during conflicts, family and gender rights, human rights infringements by technological developments, and much more.

Topic Introduction

In today's advanced digital age, we often knowingly or unknowingly give up our personal information for the sake of convenience. Whether that be letting your phone identify your location for Google Maps, accepting cookies on a website so you receive information tailored to your preferences, or accepting lengthy terms and conditions without actually knowing what you're agreeing to - we surrender our personal details on an everyday basis. But we have to ask ourselves - to what extent are we willing to give up our information for the sake of ease and comfort?

Doesn't everyone have the right to keep their information private?

What do we mean by the right to privacy?

Privacy is defined to be "an indispensable feature of a democracy where an individual maintains his identity while contributing to their civic duty". [8] In simple terms, privacy can be defined as the "right to be free from unwarranted intrusion and to keep certain matters from public view." [8] In the United Nations Declaration of Human Rights 1948, Article 12 states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." From this, it can be seen that privacy is universally regarded as a fundamental human right. In 2013, the General Assembly of the United Nations adopted the resolution 68/167 "The right to privacy in the digital age" [1] to specifically address this topic.

However, in the past, multiple institutions have been criticized for misusing individuals' private information. This includes governments, social media companies, tech companies, and many more.

Topic History

In the past, there have been multiple breaches of private information, whether that be by governments surveying unknowing civilians day-to-day lives, or social media companies like Facebook using information confidentially given to them by users and selling it to third parties and other companies.

One of the biggest revelations in terms of data privacy in the 21st-century was the one made by Edward Snowden in 2013, where he revealed highly classified information from the US National Security Agency (NSA). In these leaks, he revealed that the US government, along with multiple other governments and companies, were part of numerous massive global surveillance programs. It was revealed that American telephone companies were providing the NSA with all of their users' information and that the British spy agency (GCHQ) was intercepting the data flowing through the global internet by tapping fiber optic cables. These revelations shocked the world and generated unprecedented attention on privacy intrusions and digital security, leading to a global debate on the issue.

Another example of private data misuse can be seen in the recent allegations made against tech and social media giant Facebook. They have been accused of providing their users' private information to third parties, including companies like Microsoft, Spotify, and Apple. On one hand, Facebook has been severely criticized for disrespecting users' privacy and subsequently have attended multiple court hearings regarding this issue. However, Facebook has defended its behavior and said that "it never gave others access to personal data without people's permission and had seen no evidence that the data had been misused." They later acknowledged that [they] should have prevented third parties from being able to tap into users' data.

Topic Discussion

There are many situations in which digital services or technologies are used where individuals don't know if they are unknowingly being tracked or recorded, or whether they have any say in the matter since they are using these services.

- Healthcare:

Nowadays, healthcare facilities are expected to confidentially monitor peoples' health as well as keep them in check with any illnesses they may have. These records are now increasingly kept on online databases. However, how do we know that our health records are kept confidential and safe from hacks or other individuals that might try to misuse it? Since these records have been digitized, any individual that has a device that is connected to the healthcare facility can access it at any time, even if they are not an assigned doctor or nurse. When this data is kept private, economic harm, embarrassment, and discrimination can be avoided in both the professional and social aspects of an individual's life. Society expects healthcare facilities to keep their medical records confidential, but to what extent does an individual actually know how their data is stored?

- Police profiling:

Police databases have fingerprints of millions of civilians - but how do we know our fingerprints, which are a person's unique identifier, are kept safe? What if someone's fingerprints are misused and falsely placed at a crime scene to accuse them? Or to use it to access an individuals' secure accounts and facilities?

The same issue can arise with surveillance cameras where police can use cameras placed in buildings and streets to falsely identify someone who may resemble a criminal - or someone who may be falsely identified by a dodgy computer algorithm to resemble a criminal. While public surveillance cameras are useful in ensuring the safety and security of public places, they also mean that their owners (whether that be police or independent companies) can see people's locations and activities at all times. This poses a threat to an individual's privacy as they are always 'on the grid'

- The post-COVID world:

The emergence of the coronavirus has definitely brought a plethora of changes to our world and these changes will most likely be in place for the near future. The rapid digitalization of activities

like schooling, work, and shopping has resulted in the need for more security and virtual services.

An example of this is the introduction of infrared cameras that instantly show an individual's temperature in many airports and shopping centers across the world. While it's necessary to control the pandemic by restricting sick individuals' access to public places, it also means that everyone entering any public place is always monitored and that any health issues one might have that could affect their body temperature (whether that be COVID-19 related or not) suddenly become very public.

Another potential privacy breach that has become more prevalent since the start of COVID-19 and online schooling is the way schools manage virtual classes. In some cases when students are about to take a test, they are required to put their cameras on and show their teachers their surroundings including the room that they're in. This could even be their personal bedroom and whilst students have never had to mix their school and home lives before, now they are required to show multiple people including other students their private homes. This breach of privacy is an unprecedented one, however, many deem it necessary to ensure that students don't cheat.

Other situations and points that could be discussed:

- Phones - what can they record?

Phones are often used for confidential activities such as making purchases and accessing bank accounts. How secure is our credit card information, purchasing history, and browsing activity on these devices?

- Terms & conditions for apps or cookies for websites

A lot of times we accept cookies on a website or terms when signing up without actually knowing what they mean or reading all of them. Often, websites require you to accept cookies that state they can track your browsing activities and save this information in order to accept the website in the first place.

- Google faces a $5 billion lawsuit for tracking users in incognito mode

Another example of a breach of privacy as Google users thought that by using incognito mode, they wouldn't be tracked nor would their browsing activity be recorded. However, Google has said that they never said that they wouldn't record incognito mode users' browsing history. What

does this mean for users who thought they were secure by using the mode? Does Google ultimately have the right to track user activity since their services are being used?

Key Terms

1. **Censorship**
2. **Biometric Data**
3. **Mass Scale**
4. **Global Surveillance**
5. **Third Parties**
6. **Personal Data**
7. **Government**
8. **Surveillance**
9. **Transparency**
10. **Electronic Surveillance**
11. **Digital Communication**
12. **Digital Privacy**
13. **Freedom of Expression**
14. **Privacy**
15. **Social Media**
16. **Profiling**
17. **National Security**
18. **Hacking**
19. **Data Breach**
20. **Personal Right**
21. **Personal Security**

Key Questions

1. We often give our information willingly to social media apps like Facebook so now is it their choice on what they can do with it since we knowingly gave it to them? Or is it still in our hands?
2. Sometimes governments claim they take our personal information for the sake of national security - but to what extent do they have the right to collect and use that information?

3. To what extent are we willing to give up our private data for the sake of ease and comfort?
4. Should nations constantly amend their privacy laws as new technologies arise?
5. If an individual publicly uses social media, new technologies, and willingly gives up their personal data for the sake of ease, do they ultimately have a right to digital privacy anymore?

Citations

Have a look at these links and resolutions to get started and see what actions have been taken on this topic in previous years.

1. Resolution adopted by the General Assembly on 18 December 2013

http://undocs.org/A/RES/68/167

2. The Right to Privacy in the Digital Age (Report of the High Commissioner for Human Rights)

https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/PiratePartiesInternational.pdf

3. The right to Privacy in the Digital Age: Meeting Report

https://www.geneva-academy.ch/joomlatools-files/docman-files/ReportThe%20Right%20to%20Privacy%20in%20the%20Digital%20Age.pdf

4. How Europe's new privacy law will change the web, and more

https://www.wired.com/story/europes-new-privacy-law-will-change-the-web-and-more/

5. Privacy in a digital world

https://techcrunch.com/2019/09/26/privacy-queen-of-human-rights-in-a-digital-world/

6. The right to privacy in the digital age (by the Human Rights Council)

https://epic.org/misc/The-right-to%20privacy-in-the-digital-age.pdf

7. Right to privacy in the digital age (by the OHCHR)

https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx

8. The right to privacy in the digital age (definitions etc.)

https://www.ifla.org/files/assets/faife/ochr_privacy_ifla.pdf

9. What is Privacy? (Definitions, etc.)

https://privacyinternational.org/explainer/56/what-privacy

10. Edward Snowden: The 10 most important revelations from his leaks

https://mashable.com/2014/06/05/edward-snowden-revelations/

11. Edward Snowden: What the revelations mean to you

https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-fi les-surveillance-revelations-decoded#section/1

12. Facebook's data-sharing deals exposed

https://www.bbc.com/news/technology-46618582

13. The 15 biggest data breaches of the century

https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the -21st-century.html